

Результаты предыдущей лекции применим к одной задаче, уже рассмотренной нами ранее: к оценке величины $\pi_a(x)$, равной количеству простых чисел $p \leq x$, для которых $p+a$ также будет простым числом (здесь и всюду далее $a \geq 2$ — четное число). На лекции 4 для $\pi_a(x)$ была получена оценка вида

$$\pi_a(x) \leq \frac{x}{(\psi(x))^2} \cdot \frac{a}{\varphi(a)},$$

равномерная по $2 \leq a \leq x$; постоянная в знаменателе $\leq$ была абсолютной, хотя её значение нами не вычислялось. Асимптотика функции $\frac{1}{G(z)}$, найденная на предыдущей лекции, позволяет получить для $\pi_a(x)$ верхнюю оценку явно вычисленной константой. Такая задача представляет определенный интерес в связи с применением к другим задачам теории чисел. В их числе — теорема П. Эрмита о существовании бесконечного множества пар соседних простых чисел p_n, p_{n+1} для которых разность $p_{n+1} - p_n$ "мала" по сравнению со "средним" значением $\psi(p_n)$.

Теорема 1. Пусть $x \geq x_0 > 2$, $2 \leq a \leq x$ — произвольное четное число. Тогда

$$\pi_a(x) \leq 4C_0 \kappa(a) \frac{x}{(\psi(x))^2} \left(1 + O\left(\frac{\psi(a)a}{\psi(x)}\right) \right),$$

где $C_0 = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2} \right)$.

Замечание. Правая часть отличается от ожидаемой асимптотически лишь множителем 4.

2-во. Возьмем в качестве P множество всех простых чисел, не делящих a , и имеем

$$a_n = \begin{cases} 1, & \text{если } n = p+a, p \in \pi - \text{простое;} \\ 0, & \text{в противном случае.} \end{cases}$$

Предполагая $2 \leq z \leq \sqrt{x+a}$, рассмотрим просеивающую функцию $S(A, P, z)$. Она выражает количество простых $p \leq x$, для которых $(p+a, P(z)) = 1$, где $P(z) = \prod_{p \leq z, p \nmid a}$. В сумме S , таким образом,

не учитываются возможные простые числа $p < z$, для которых $p+a$ — простое и $p+a < z$. Но их количество, очевидно, не превышает z , так что

$$\pi_a(x) \leq S(A, P, z) + z.$$

Далее, $|A_d| = \sum_{p \leq x, p+a \equiv 0 \pmod{d}} 1 = \pi(x, d, -a).$

Если $(d, a) > 1$, то $|A_d| \equiv 0$ кроме, быть может, случая, когда a — простое (т.е. $a=2$) и $d=2$ (и тогда $|A_d| \equiv 1$). Если же $(d, a) = 1$, то

$$|A_d| = \frac{Li(x)}{\varphi(d)} + R(x, d, -a),$$

и, таким образом

$$X = Li(x) = \frac{x}{\ln x} + O\left(\frac{x}{\ln^2 x}\right), \quad g(d) = \begin{cases} \frac{1}{\varphi(d)}, & (d, a) = 1 \\ 0, & (d, a) > 1 \end{cases}$$

В силу неравенства решета Селберга,

$$S(A, P, z) \leq \frac{X}{G(z)} + R,$$

где $R \leq 1 + \sum_{\substack{d \leq z^2 \\ d \nmid P(z)}} 3\omega(d) |R(x, d, -a)|.$

Величину R оценим с помощью теоремы Бомбieri-Виноградова (вспомогательная лемма 6). Теорема Э. Бомбieri и А. И. Виноградова утверждает следующее.

Какова бы ни была постоянная $A > 0$, найдется постоянная B , зависящая лишь от A и такая, что при всех достаточно больших $x \geq x_0$ справедлива оценка:

$$\sum_{\substack{q \leq \frac{\sqrt{x}}{(Cx)^B}}} \max_{y \leq x} \left| \max_{(a,q)=1} R(x; q, a) \right| \leq \frac{C_0 x}{(Cx)^A}$$

Здесь x_0 — некоторая неэффективная постоянная (неэффективность означает в данном случае невозможность указать алгоритм, который по заданному A смог бы вычислить значение x_0). Зависимость B от A может быть указана явно; например в настоящей работе результат отвечает $B = A + \frac{5}{2}$.

Прежде всего, заметим, что

$$R(x, d, -a) = \pi(x, d, -a) - \frac{Li(x)}{\varphi(d)} \leq \frac{x}{d} + 1 - \frac{Li(x)}{d} \leq \frac{2x}{d} \quad \text{и}$$

$$R(x, d, -a) \geq -\frac{Li(x)}{\varphi(d)} = -\frac{x}{d} \cdot \frac{d}{\varphi(d)} \cdot \frac{Li(x)}{x} \geq -\frac{x}{d} \cdot \frac{2 \ln \ln d}{\ln x} \geq -\frac{x}{d}, \quad \text{так что } |R(x, d, -a)| \leq \frac{2x}{d}$$

при всех d , $1 \leq d \leq x$. Отсюда, предполагая, что $z^2 \leq \frac{\sqrt{x}}{(Cx)^B}$ (B — постоянная, значение которой будет указано ниже), получим:

$$R \leq \sum_{d \leq z^2} \tau_3(d) \sqrt{|R(x, d, -a)|} \sqrt{|R(x, d, -a)|} \leq$$

$$\leq \sum_{d \leq z^2} \tau_3(d) \sqrt{\frac{2x}{d}} \sqrt{|R(x, d, -a)|}, \quad \text{откуда, в силу}$$

неравенства Коши, найдём:

$$R \leq \sqrt{2x} \left(\sum_{d \leq z^2} \frac{\tau_3^2(d)}{d} \right)^{\frac{1}{2}} \left(\sum_{d \leq z^2} |R(x, d, -a)| \right)^{\frac{1}{2}} \ll$$

$$\ll \sqrt{x} \left((Cx)^{3^2} \right)^{\frac{1}{2}} \left(\frac{x}{(Cx)^A} \right)^{\frac{1}{2}} \ll \frac{x}{(Cx)^{\frac{1}{2}(A-9)}}$$

Беря $A = 15$, $B = A + 5/2 = 35/2$, для $z^2 \leq \sqrt{x} (Cx)^{-\frac{35}{2}}$, приходим к оценке $R \ll \frac{x}{(Cx)^3}$.

Переходим теперь к вычислению величины $\frac{1}{G(z)}$. Если $p \nmid a$, то p — нечетное и, т.о.,

$$g(p) = \frac{1}{p-1} \leq \frac{1}{2} = 1 - \frac{1}{2},$$

так что условие g_1 выполнено с $A_1 = 2$. Далее, для проверки условия $g_2(x; L)$ заметим, что при всех $x > 1$ выполняются неравенства

$$v_x - E - \frac{1}{2v_x} < \sum_{p \in x} \frac{v_p}{p} < v_x,$$

где $E = 1, 0, \dots$ — постоянная (это Теорема Бассе вследствие из уже упоминавшейся работы Россера и Шенфельда). Итак, пусть $2 \leq u < v$. Тогда

$$S = \sum_{u < p \leq v} g(p)(v_p) = \sum_{\substack{u < p \leq v \\ p \nmid a}} \frac{v_p}{p-1} = \sum_{\substack{u < p \leq v \\ p \nmid a}} \left(\frac{v_p}{p} + \frac{v_p}{p(p-1)} \right),$$

$$\text{откуда } S < \sum_{u < p \leq v} \frac{v_p}{p} + \sum_{p \geq 2} \frac{v_p}{p(p-1)} < v_v - v_u + E + \frac{1}{2v_u} +$$

$$+ \sum_{p \geq 2} \frac{v_p}{p(p-1)} \leq v_v - \frac{v}{u} + A_2, \quad A_2 = E + \frac{1}{2v_2} + \sum_{p \geq 2} \frac{v_p}{p(p-1)}.$$

$$\text{Далее,}$$

$$S > \sum_{u < p \leq v} \frac{v_p}{p} - \sum_{p \mid a} \frac{v_p}{p} > v_v - E - \frac{1}{2v_v} - v_u - \sum_{p \mid a} \frac{v_p}{p}$$

$$\geq v_v - \frac{v}{u} - E - \frac{1}{2v_2} - \sum_{p \mid a} \frac{v_p}{p}.$$

Заметим, что при любых $\gamma > e$ справедливы неравенства

$$\sum_{p \mid a} \frac{v_p}{p} = \left(\sum_{\substack{p \mid a \\ p \leq \gamma}} + \sum_{\substack{p \mid a \\ p > \gamma}} \right) \frac{v_p}{p} \leq \sum_{p \leq \gamma} \frac{v_p}{p} +$$

$$+ \frac{v_\gamma}{\gamma} \sum_{p \mid a} 1 < v_\gamma + \omega(a) \frac{v_\gamma}{\gamma}.$$

Беря теперь $\gamma = v_a$, и замечая, что $\omega(a) \ll \frac{v_a}{v_a}$, находим:

$$\sum_{p \mid a} \frac{v_p}{p} < v_a + O(1), \text{ откуда}$$

$$S > v_v - \frac{v}{u} - L, \quad L = v_a + O(1),$$

где постоянная в знаке O — абсолютная.

Итак, условие $g_2(x; L)$ выполнено с $x=1$, $L = \ln \ln a + O(1)$.

Применяя теорему с краинной леммой, находим:

$$\frac{1}{G(z)} = V(z) e^{\gamma} \Gamma(2) \left(1 + O\left(\frac{\ln \ln a}{a z}\right)\right) = e^{\gamma} V(z) \left(1 + O\left(\frac{\ln \ln a}{a z}\right)\right),$$

$$V(z) = \prod_{p \leq z, p \nmid a} \left(1 - \frac{1}{p-1}\right).$$

Величину $V(z)$ преобразуем, опираясь на формулу Мертенса. Имено,

$$V(z) = \prod_{3 \leq p \leq z} \left(1 - \frac{1}{p-1}\right) \prod_{\substack{3 \leq p \leq z \\ p \nmid a}} \frac{p-1}{p-2} \leq x(a) \prod_{3 \leq p \leq z} \left(1 - \frac{1}{p-1}\right),$$

где $x(a) = \prod_{p \nmid a, p \geq 3} \frac{p-1}{p-2}$. Далее, при $p \geq 3$ имеем:

$$1 - \frac{1}{p-1} = \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{(p-1)^2}\right), \quad \text{так что}$$

$$V(z) = x(a) \prod_{3 \leq p \leq z} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{(p-1)^2}\right) = 2x(a) \prod_{p \leq z} \left(1 - \frac{1}{p}\right) \cdot$$

$$\cdot \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} = 2C_0 x(a) \prod_{p \leq z} \left(1 - \frac{1}{p}\right) \cdot$$

$$\cdot \left\{1 + O\left(\frac{1}{z \ln z}\right)\right\} = C_0 e^{-\gamma} \frac{x(a)}{a z} \left\{1 + O\left(\frac{1}{a z}\right)\right\},$$

где $C_0 = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right)$. Итак,

$$\frac{1}{G(z)} \leq e^{\gamma} C_0 e^{-\gamma} \frac{x(a)}{a z} \left(1 + O\left(\frac{\ln \ln a}{a z}\right)\right) =$$

$$= \frac{C_0 x(a)}{a z} \left(1 + O\left(\frac{\ln \ln a}{a z}\right)\right).$$

Собирая полученные оценки вместе, приходим к неравенству

$$\pi_a(x) \leq \frac{C_0 x(a)}{a z} \cdot \frac{x}{a x} \left(1 + O\left(\frac{\ln \ln a}{a z}\right)\right) + O\left(\frac{x}{(a x)^3}\right),$$

где $z^2 \leq \sqrt{x} (a x)^{-B}$. Полагая $z = x^{1/4} (a x)^{-B/2}$,

придем к искомым утверждению.

Оценку теоремы 1 мы используем для доказательства следующей теоремы Эрдёша.

Теорема 2 Для любой постоянной ε , $0 < \varepsilon < \frac{1}{8}$, существует бесконечная последовательность пар соседних простых чисел p_n, p_{n+1} , для которых $p_{n+1} - p_n \leq (\frac{7}{8} + \varepsilon) \psi(p_n)$.

Д-во Зададимся произвольным δ , $0 < \delta < 1$, и предположим, что при всех $X \geq X_0(\delta)$ и всех p , $X < p \leq 2X$, верно неравенство:

$$d_n = p_{n+1} - p_n > (1 - \delta) \psi(X).$$

Покажем, что это приводит к противоречию, если δ достаточно мало. Для этого рассмотрим сумму

$$W = \sum_{X < p_n \leq 2X} d_n.$$

В силу асимптотического закона, $W = X + O(Xe^{-\sqrt{\log X}})$. Пусть, далее, $a \geq 2$ — четное число, и $v(a) = v(a; X)$ — количество простых p_n с условиями $p_{n+1} - p_n = a$, $X < p_n \leq 2X$.

Тогда, очевидно,

$$\sum_{a \geq 2} v(a) = \pi(2X) - \pi(X) = \pi_1(X) = \frac{X}{\psi(X)} + O\left(\frac{X}{(\log X)^2}\right),$$

причем $v(a) = 0$ при $2 \leq a \leq (1 - \delta) \psi(X) = L_1$.

Положим $L_2 = (1 + \delta) \psi(X)$, преобразуем W следующим образом:

$$W = \sum_{a > L_1} a v(a) = \left(\sum_{L_1 < a \leq L_2} + \sum_{a > L_2} \right) a v(a) \geq$$

$$\geq \sum_{L_1 < a \leq L_2} a v(a) + L_2 \sum_{a > L_2} v(a) = \sum_{L_1 < a \leq L_2} a v(a) +$$

$$+ L_2 \left(\sum_{a > L_1} - \sum_{L_1 < a \leq L_2} \right) v(a) = \sum_{L_1 < a \leq L_2} a v(a) -$$

$$- L_2 \sum_{L_1 < a \leq L_2} v(a) + L_2 \pi_1(X) = \pi_1(X) L_2 - \sum_{L_1 < a \leq L_2} (L_2 - a) v(a).$$

Для всех a , $L_1 < a \leq L_2$, имеем: $L_2 - a > 0$. Далее, в силу теоремы 1 имеем:

$$v(a) \leq 4C_0 x(a) \frac{X}{(LX)^2} \left(1 + O\left(\frac{1}{LX}\right)\right)$$

Следовательно,

$$W \geq \pi_1(X) L_2 - \frac{4C_0 X}{(LX)^2} \left(1 + O\left(\frac{1}{LX}\right)\right) \sum_{L_1 < a \leq L_2} (L_2 - a) \cdot x(a).$$

Возмем сумму

$$W_1 = \sum_{L_1 < a \leq L_2} x(a), \quad W_2 = \sum_{L_1 < a \leq L_2} a x(a).$$

по определению,

$$x(a) = \prod_{p|a, p \geq 3} \frac{p-1}{p-2} = \prod_{p|a, p \geq 3} (1 + h(p)), \quad h(p) = \frac{1}{p-2},$$

так что

$x(a) = \sum'_{d|a} \mu^2(d) h(d)$, где $\sum'$ означает суммирование по нечетным делителям a . Соответственно, полагая

$W(x) = \sum'_{a \leq x} x(a)$ (двойное $\sum'$ здесь и далее означает суммирование по четным числам $a \geq 2$), будем иметь:

$$\begin{aligned} W(x) &= \sum'_{a \leq x} \sum'_{d|a} \mu^2(d) h(d) = \sum'_{d \leq x} \mu^2(d) h(d) \sum'_{\substack{a \leq x \\ a \equiv 0 \pmod{d}}} 1 = \\ &= \sum'_{d \leq x} \mu^2(d) h(d) \sum'_{\substack{a \leq x \\ a \equiv 0 \pmod{2d}}} 1 = \sum'_{d \leq x} \mu^2(d) h(d) \left[\frac{x}{2d} \right] = \\ &= \frac{x}{2} \sum'_{d \leq x} \mu^2(d) \frac{h(d)}{d} + O_1 \sum'_{d \leq x} \mu^2(d) h(d). \end{aligned}$$

Оценим сначала последнюю сумму, обозначаемую далее $V(x)$. Для этого заметим следующее. Пусть $p \geq 3$ — простое. Представим $h(p)$ в виде

$$h(p) = \frac{1}{p} \cdot \frac{1}{1 - \frac{2}{p}} = \frac{1}{p} \left(1 + \frac{2}{p-2}\right) = \frac{1}{p} \left(1 + \frac{2}{p} + \frac{4}{p(p-2)}\right) =$$

$$= \frac{1}{p} \left(1 + \frac{2}{p}\right) \left(1 + \frac{4}{(p-2)(p+2)}\right) = \frac{1}{p} \left(1 + \frac{2}{p}\right) \left(1 + \frac{4}{p^2-4}\right).$$

Следовательно, для каждого бесквадратного d имеем:

$$h(d) = \prod_{p|d} \frac{1}{p} \left(1 + \frac{2}{p}\right) \left(1 + \frac{4}{p^2-4}\right) = \frac{1}{d} \prod_{p|d} \left(1 + \frac{2}{p}\right) \prod_{p|d} \left(1 + \frac{4}{p^2-4}\right)$$

$$< \frac{1}{d} \prod_{p \geq 3} \left(1 + \frac{4}{p^2-4}\right) \prod_{p|d} \left(1 + \frac{2}{p}\right) = \frac{C}{d} \sum_{\delta|d} \frac{2^{\omega(\delta)}}{\delta}, \text{ где}$$

$$C = \prod_{p \geq 3} \left(1 + \frac{4}{p^2-4}\right) - \text{абсолютная постоянная.}$$

Значит,

$$V(x) < C \sum'_{d \leq x} \frac{\mu^2(d)}{d} \sum_{\delta|d} \frac{2^{\omega(\delta)}}{\delta} = C \sum'_{\delta \leq x} \frac{2^{\omega(\delta)}}{\delta} \sum_{d \leq x} \frac{\mu^2(d)}{d}$$

$$= C \sum'_{\delta \leq x} \frac{2^{\omega(\delta)}}{\delta} \sum_{\substack{h \leq \frac{x}{\delta} \\ (h, \delta) = 1}} \frac{\mu^2(h) \mu^2(\delta)}{h \delta} \leq C \sum'_{\delta \leq x} \frac{\mu^2(\delta)}{\delta^2} 2^{\omega(\delta)} \sum_{\substack{h \leq \frac{x}{\delta} \\ d \equiv 0 \pmod{\delta}}} \frac{\mu^2(h)}{h}$$

$$\leq C \sum'_{\delta \leq x} \frac{\mu^2(\delta)}{\delta} 2^{\omega(\delta)} \left(e^{\frac{x}{\delta}} + 1 \right) \leq C(e x + 1) \sum_{\delta=1}^{+\infty} \frac{\mu^2(\delta)}{\delta} 2^{\omega(\delta)}$$

$\ll e x$, так что

$$W(x) = \frac{x}{2} \left(\sum_{d=1}^{+\infty} \mu^2(d) \frac{h(d)}{d} - \sum_{d>x} \mu^2(d) \frac{h(d)}{d} \right) + O(e x).$$

В силу конечности верхней оценки $h(d)$ имеем:

$$\sum_{d>x} \mu^2(d) \frac{h(d)}{d} < C \sum'_{d>x} \frac{\mu^2(d)}{d^2} \sum_{\delta|d} \frac{2^{\omega(\delta)}}{\delta} \leq$$

$$\leq C \sum_{d>x} \frac{\mu^2(d)}{d^2} \sum_{\delta|d} \frac{\tau(\delta)}{\delta} \leq C \sum_{d>x} \frac{\mu^2(d)}{d^2} \tau_3(d) \leq$$

$$\leq C \sum_{d>x} \frac{\tau_3(d)}{d^2} \ll \frac{(e x)^2}{x}, \text{ и потому}$$

$$W(x) = \frac{x}{2} \sum_{d=1}^{+\infty} \mu^2(d) \frac{h(d)}{d} + O((e x)^2),$$

Канонич., в силу мультипликативности $h(d)$ каждого:

$$\frac{1}{2} \sum_{d=1}^{+\infty} \chi^2(d) \frac{h(d)}{d} = \frac{1}{2} \prod_{p \geq 3} \left(1 + \frac{h(p)}{p}\right) = \frac{1}{2} \prod_{p \geq 3} \left(1 + \frac{1}{p(p-2)}\right) =$$

$$= \frac{1}{2} \prod_{p \geq 3} \frac{(p-1)^2}{p(p-2)} = C_1, \quad W(x) = C_1 x + O(e^2 x),$$

Применяя преобразование Абеля, заключаем:

$$\sum_{a \leq x} a \chi(a) = x W(x) - \int_1^x W(u) du = x(C_1 x + O(e^2 x)) - \int_1^x (C_1 u + O((e u)^2)) du =$$

$$= C_1 x^2 - C_1 \frac{u^2}{2} \Big|_1^x + O(x(e x)^2) = \frac{1}{2} C_1 x^2 + O(x(e x)^2).$$

Возвращаясь к сумме W_1 и W_2 , находим:

$$W_1 = C_1 L_2 - C_1 L_1 + O(e^2 L_2) = C_1 (L_2 - L_1) + O(e^2 L_2) =$$

$$= C_1 \cdot 2\delta e x + O((e e x)^2),$$

$$W_2 = \frac{1}{2} C_1 (L_2^2 - L_1^2) + O((e x)(e e x)^2) =$$

$$= \frac{1}{2} C_1 \cdot 2\delta (e x) \cdot 2(e x) + O((e x)(e e x)^2) =$$

$$= 2\delta C_1 (e x)^2 + O((e x)(e e x)^2),$$

Итак,

$$\sum_{L_1 < a \leq L_2} (L_2 - a) \chi(a) = L_2 W_1 - W_2 = (1 + \delta)(e x) W_1 - W_2 =$$

$$= 2\delta(1 + \delta) C_1 (e x)^2 - 2\delta C_1 (e x)^2 + O((e x)(e e x)^2) =$$

$$= 2\delta^2 C_1 (e x)^2 + O((e x)(e e x)^2).$$

Получим:

$$W \geq \pi_1(x) L_2 - \frac{4 C_1 x}{(e x)^2} \left\{ 1 + O\left(\frac{1}{e x}\right) \right\} \times (2\delta^2 C_1 (e x)^2 +$$

$$+ O((e x)(e e x)^2)) = (1 + \delta) x \left(1 + O\left(\frac{1}{e x}\right)\right) -$$

$$- 8\delta^2 C_1 X \left(1 + O\left(\frac{(a_n X)^2}{a_n X}\right) \right) = (1 + \delta - 8\delta^2 C_1) X \left(1 + O\left(\frac{(a_n X)^2}{a_n X}\right) \right)$$

Заметим теперь, что

$$C_1 = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2} \right) \cdot \frac{1}{2} \prod_{p \geq 3} \frac{(p-1)^2}{p(p-2)} \equiv 1.$$

Следовательно,

$$W \geq (1 + \delta - 8\delta^2) X \left(1 + O\left(\frac{(a_n X)^2}{a_n X}\right) \right)$$

Возьмем теперь $\delta = \frac{1}{8} - \varepsilon$, где $0 < \varepsilon < \frac{1}{8}$. Тогда

$$\delta - 8\delta^2 = \frac{1}{8} - \varepsilon - 8\left(\frac{1}{64} - \frac{\varepsilon}{4} + \varepsilon^2\right) = \varepsilon - 8\varepsilon^2 > 0,$$

$1 + \delta - 8\delta^2 \geq 1 + \varepsilon - 8\varepsilon^2 > 1$, так что при всех достаточно больших X получим:

$$W \geq \left(1 + \frac{1}{2}(\varepsilon - 8\varepsilon^2)\right) X,$$

что противоречит соотношению

$$W = X + O(X e^{-c\sqrt{a_n X}}).$$

Итак, существует бесконечно много пар соседних простых чисел p_n, p_{n+1} таких, что

$$p_{n+1} - p_n \leq \left(\frac{7}{8} + \varepsilon\right) p_n.$$

Теорема 2 доказана.

Укажем ещё одно применение теоремы Крамной леммы, связанное с подсчётом числа тех $n \leq x$, для которых значения заданных полиномов $F_1(x), \dots, F_r(x)$ при $x = n$ все будут простыми числами. Соответствующая теорема, однако, опирается на один глубокий факт теории алгебраических чисел — теорему Ландау о простых идеалах:

Пусть K — поле алгебраических чисел конечной степени над $\mathbb{Q}$, и пусть $\mathcal{O}_K$ — кольцо алгебраических целых чисел K . Тогда количество простых идеалов $\mathfrak{p}$ в $\mathcal{O}_K$ с условием $N(\mathfrak{p}) \leq x$ при $x \rightarrow +\infty$ выражается асимптотической формулой

$$Li(x) + O(x e^{-c\sqrt{\log x}}), \quad c = c(K) > 0.$$

Эта теорема была доказана в статье: E. Landau, Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes, Math. Annalen, 56 (1903), №4, s. 645-670. Подробное изложение содержится в книге: E. Landau, Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, Leipzig und Berlin, 1918 (Satz 190, 191).

Следствием этой теоремы, необходимым для наших целей, является

Лемма 1. Пусть $f(x)$ — неприводимый многочлен степени $n \geq 1$ с целыми коэффициентами, и пусть $\rho_f(p)$ — число решений сравнения $f(x) \equiv 0 \pmod{p}$ с условиями $0 \leq x \leq p-1$. Тогда при $w \rightarrow +\infty$ справедлива следующая асимптотическая формула:

$$\sum_{p \leq w} \frac{\rho_f(p)}{p} = \kappa_f \ln w + c(f) + O\left(\frac{1}{\ln^2 w}\right),$$

где $c(f)$ — некоторая постоянная.

Это утверждение мы оставляем без доказательства.

Также нам потребуется

Лемма 2. Пусть $F_1(x), \dots, F_r(x)$ — различные неприводимые многочлены с целыми коэффициентами, и пусть $\rho_{F_i}(p)$ — число решений сравнения $F_i(x) \equiv 0 \pmod{p}$, $0 \leq x \leq p-1$. Тогда, положив $F(x) = F_1(x) \dots F_r(x)$, для всех простых $p \geq p_0(F)$ имеем:

$$\rho_F(p) = \rho_{F_1}(p) + \dots + \rho_{F_r}(p).$$

Д-во. Достаточно проверить, что для всех достаточно больших p одновременная делимость на p чисел $F_i(n)$, $F_j(n)$ (n — некоторое целое) невозможна. Действительно, пусть $1 \leq i < j \leq r$, и пусть для некоторого простого p и некоторого целого n оказалось: $F_i(n) \equiv 0 \pmod{p}$, $F_j(n) \equiv 0 \pmod{p}$, или, что то же, $p \mid F_i(n)$, $p \mid F_j(n)$. Но тогда $p \mid (F_i(n), F_j(n))$, поскольку F_i, F_j неприводимы

и различны, то F_i и F_j взаимно просты. Следовательно, найдутся многочлены $P(x), Q(x) \in \mathbb{Q}[x]$ такие, что $F_i(x)P(x) + F_j(x)Q(x) \equiv 1$. Многочлен на соответствующее целое число c_{ij} зависящее лишь от F_i и F_j , получим:

$$F_i(x)P_1(x) + F_j(x)Q_1(x) = c_{ij},$$

где $P_1, Q_1 \in \mathbb{Z}[x]$. Положив $x = u$, получим: $p \mid c_{ij}$. Следовательно, все простые, для которых сравнения $F_i(x) \equiv 0 \pmod{p}$, $F_j(x) \equiv 0 \pmod{p}$, $1 \leq i < j \leq r$ имеют общие решения, являются делителями числа $c = \prod_{1 \leq i < j \leq r} c_{ij}$, зависящего лишь от $F_1, \dots, F_r$. лемма доказана.

Теорема 3 Пусть $F_1, \dots, F_r$ — различные неприводимые многочлены с целыми коэффициентами, причем их старшие коэффициенты положительны, $F(x) = F_1(x) \dots F_r(x)$, $r(p)$ — число решений сравнения $F(x) \equiv 0 \pmod{p}$, $0 \leq x \leq p-1$. Пусть, далее, $0 \leq r(p) \leq p-1$ для всех простых p . Тогда для числа $N(x) = N(x; F_1, \dots, F_r)$ целых x , $1 \leq x \leq x$, для которых все числа $F_1(x), \dots, F_r(x)$ будут простыми, справедлива следующая оценка:

$$N(x) \leq 2^r \cdot r! \cdot C(F) \cdot \frac{x}{(C(x))^r} \left\{ 1 + O_F \left(\frac{C(x)}{C(x)} \right) \right\},$$

где
$$C(F) = \prod_p \left(1 - \frac{r(p)-1}{p-1} \right) \left(1 - \frac{1}{p} \right)^{-(r-1)}$$

2-во Проверим выполнение условий $g \rightarrow g_1, \dots, g_r(x; L)$ для этого положим

$$a_n = \begin{cases} 1, & \text{если } n = F(m) \text{ при некотором } m, \quad 1 \leq m \leq x; \\ 0, & \text{в противном случае.} \end{cases}$$

Возьмем в качестве P множество всех простых чисел $\mathbb{P}$, имеем тогда:

$$|Ad| = \sum_{1 \leq m \leq x} 1 = \left[\frac{x}{d} \right] r(d) + O_r(d) =$$

$$F(m) \equiv 0 \pmod{d}$$

$$= \frac{x}{d} p(d) + \theta_2 p(d), \text{ где } 0 \leq \theta_1 \leq 1, -1 \leq \theta_2 \leq 1. \text{ Итак,}$$

$X = x$, $g(d) = \frac{p(d)}{d}$, $\tau_d = \theta_2 p(d)$. Далее, если p - простое, то, полагая $n = \deg F = \sum_{i=1}^n \deg F_i$, при $p \geq n+1$ получим из теоремы Лагранжа:

$$0 \leq g(p) = \frac{p(p)}{p} \leq \frac{n}{p} \leq \frac{n}{n+1} = 1 - \frac{1}{n+1}.$$

Всего же $p \leq n$, то в силу предположения $g(p) \leq p-1$, так что

$$0 \leq g(p) \leq \frac{p-1}{p} = 1 - \frac{1}{p} \leq 1 - \frac{1}{n}.$$

Следовательно, условие g_1 выполнено с постоянной $A_1 = n+1$.

Далее, пусть $p \geq p_0(F)$. Тогда, в силу леммы 2

$$g(p) = g_{F_1}(p) + \dots + g_{F_r}(p),$$

Далее, из леммы 1 заключаем:

$$C_i(w) = \sum_{p \leq w} \frac{g_{F_i}(p)}{p} = a_i \ln w + c_i + O\left(\frac{1}{\ln^2 w}\right),$$

$$\text{откуда } \sum_{p \leq w} \frac{g_{F_i}(p)}{p} a_i p = \left(a_i \ln w + c_i + O\left(\frac{1}{\ln^2 w}\right)\right) a_i w -$$

$$- \int_{3/2}^w \left(a_i \ln u + c_i + O\left(\frac{1}{\ln^2 u}\right)\right) \frac{du}{u} = \int_{3/2}^w \frac{a_i u}{u \ln u} du -$$

$$- \int_{3/2}^{+\infty} O\left(\frac{1}{\ln^2 u}\right) \frac{du}{u} + \int_w^{+\infty} O\left(\frac{1}{\ln^2 u}\right) \frac{du}{u} + O\left(\frac{1}{\ln w}\right) =$$

$= a_i w + c_i + O\left(\frac{1}{\ln w}\right)$, где c_i - некоторая постоянная, зависящая лишь от полинома $F_i(x)$. Итак,

$$\sum_{p \leq w} \frac{g(p)}{p} a_i p = \sum_{p \leq p_0} \frac{g(p)}{p} a_i p + \sum_{p_0 < p \leq w} \frac{g(p)}{p} a_i p =$$

$$\begin{aligned}
&= \sum_{p \leq p_0} \frac{s(p)}{p} \ln p + \sum_{p_0 < p \leq w} \sum_{i=1}^r \frac{s_{F_i}(p)}{p} \ln p = \\
&= \sum_{i=1}^r \left(\sum_{p \leq w} \frac{s_{F_i}(p)}{p} \ln p \right) + \sum_{p \leq p_0} \frac{s(p)}{p} \ln p - \\
&- \sum_{i=1}^r \left(\sum_{p \leq p_0} \frac{s_{F_i}(p)}{p} \ln p \right) = \sum_{i=1}^r \left(\sum_{p \leq w} \frac{s_{F_i}(p)}{p} \ln p \right) + \\
&+ G(F) = r \ln w + (G_1 + \dots + G_r) + G(F) + O\left(\frac{1}{\ln w}\right) = \\
&= r \ln w + A + O\left(\frac{1}{\ln w}\right), \text{ где константная } A \text{ зависит} \\
&\text{только от } F_1, \dots, F_r. \text{ Итак, условие } g_2(x, L) \text{ выполнено} \\
&\text{если } x = x, \quad L = O_F(1). \quad \square
\end{aligned}$$

Следовательно,

$$N(x) \leq \frac{x}{G(x)} + R \leq x e^{r\delta} \Gamma(r+1) V(x) \left(1 + O\left(\frac{1}{\ln x}\right)\right) + R,$$

$$\text{где } V(x) = \prod_{p \leq x} \left(1 - \frac{s(p)}{p}\right), \quad R = \sum_{d < x^2} s(d).$$

Заметим, что в силу теоремы Лагранжа $s(d) \leq n^{\omega(d)} \leq \tau_n(d)$ при всех d , так что

$$R \ll x^2 (\ln x)^{n-1} \ll x^2 (\ln x)^{n-1}.$$

Далее,

$$\begin{aligned}
V(x) &= \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^r \prod_{p \leq x} \left(1 - \frac{s(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-r} = \\
&= \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^r \prod_p \left(1 - \frac{s(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-r} \prod_{p > x} \left(1 - \frac{s(p)}{p}\right) \left(1 - \frac{1}{p}\right)^r
\end{aligned}$$

В силу формулы Мертенса, первое произведение есть

$$\frac{e^{-\delta x}}{(\ln x)^r} \left(1 + O\left(\frac{1}{\ln x}\right)\right).$$

Последнее произведение есть

$$\exp \left\{ \sum_{p > x} \left(r \ln \left(1 - \frac{1}{p}\right) - \ln \left(1 - \frac{s(p)}{p}\right) \right) \right\} = \exp \left\{ \sum_{p > x} \frac{s(p) - r}{p} + \right.$$

$$+ O\left(\sum_{p \geq z} \frac{1}{p^2}\right)\} \quad \text{но имеем (при } z > p_0(F))$$

$$\sum_{p \geq z} \frac{\rho(p) - \tau}{p} = \lim_{y \rightarrow +\infty} \left\{ \sum_{z < p \leq y} \frac{\rho(p)}{p} - \tau \sum_{z < p \leq y} \frac{1}{p} \right\} =$$

$$= \lim_{y \rightarrow +\infty} \left\{ \tau \ln y - \tau \ln z + O\left(\frac{1}{az}\right) - \tau \ln y + \tau \ln z + \right.$$

$$\left. + O\left(\frac{1}{az}\right) \right\} = O\left(\frac{1}{az}\right), \quad \text{так что}$$

$$V(z) = \frac{e^{-\tau z}}{(az)^{\tau}} C \left(1 + O\left(\frac{1}{az}\right)\right), \quad \text{где}$$

$$C = \prod_p \left(1 - \frac{\rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-\tau} \quad - \text{постоянная.}$$

Заметим также:

$$\left(1 - \frac{\rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-\tau} = \left(1 - \frac{\rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^{1-\tau} =$$

$$= \left(1 - \frac{\rho(p)-1}{p-1}\right) \cdot \frac{p-1}{p-\rho(p)} \cdot \left(1 - \frac{\rho(p)}{p}\right) \frac{p}{p-1} \left(1 - \frac{1}{p}\right)^{1-\tau} =$$

$$= \left(1 - \frac{\rho(p)-1}{p-1}\right) \left(1 - \frac{1}{p}\right)^{1-\tau}, \quad \text{так что}$$

$$C = \prod_p \left(1 - \frac{\rho(p)-1}{p-1}\right) \left(1 - \frac{1}{p}\right)^{-(\tau-1)}$$

Собирая полученные выражения, найдём:

$$N(x) \leq \frac{x \cdot \tau!}{(az)^{\tau}} C \left(1 + O\left(\frac{1}{az}\right)\right) + z^2 (az)^{\tau},$$

полагая $z = x^{\frac{1}{2}} (ax)^{-B}$, где $B = B(\tau)$, приходим к неравенству:

$$N(x) \leq 2^{\tau} \tau! C \frac{x}{(ax)^{\tau}} \left(1 + O\left(\frac{ax}{ax}\right)\right),$$

где постоянная в знаке O зависит от F .

Теорема 3 доказана.

Приведем несколько следствий теоремы 3.

Следствие 1 Множество N_1 чисел n , $1 \leq n \leq x$, для которых числа n^2+1 , n^2+3 — простые, удовлетворяет неравенству:

$$N_1 \leq 32 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \equiv \pm 1 \pmod{12}} \left(1 - \frac{2\varepsilon(p)}{p-2}\right) \frac{x}{(ex)^2} \times \\ \times \left(1 + O\left(\frac{e_n e_x}{a x}\right)\right),$$

где $\varepsilon(p) = \begin{cases} 1, & p \equiv 1 \pmod{12}, \\ -1, & p \equiv -1 \pmod{12} \end{cases}$

Следствие 2 Множество N_2 чисел n , $1 \leq n \leq x$, для которых числа n^2-2n+2 , n^2+2n+2 — простые, удовлетворяет неравенству

$$N_2 \leq 16 \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p > 2} \left(1 - \frac{2(-1)^{\frac{p-1}{2}}}{p-2}\right) \frac{x}{(ex)^2} \left(1 + O\left(\frac{e_n e_x}{a x}\right)\right)$$

Следствие 3 Пусть $F(x)$ — неприводимый полином с целыми коэффициентами и положительным старшим коэффициентом, $r(p)$ — число решений сравнения $F(x) \equiv 0 \pmod{p}$, $0 \leq x \leq p-1$. Пусть, далее, $0 \leq r(p) \leq p-1$ для всякого простого p . Тогда множество N_3 чисел n , $1 \leq n \leq x$, для которых $F(n)$ — простое число, удовлетворяет при $x \rightarrow +\infty$ неравенству:

$$N_3(x) \leq 2 \prod_p \left(1 - \frac{r(p)-1}{p-1}\right) \frac{x}{e_n x} \left(1 + O_F\left(\frac{e_n e_x}{a x}\right)\right).$$

Все эти утверждения остаются для самостоятельной проверки. Также рекомендуется рассмотреть последнее утверждение в частном случае $F(x) = x^2 + a$ (где $a \neq -b^2$ — целое),

$F(x) = x^4 + 1$, а также получить с помощью теоремы 3 верхнюю оценку числа тех простых p , $2 < p \leq x$, для которых все числа

$p_1 = p-2$, $p_2 = p+4$ — $p_3 = p+6$ — простые (обобщение задачи о простых близнецах).